McAfee
個人情報の盗難を防止するために

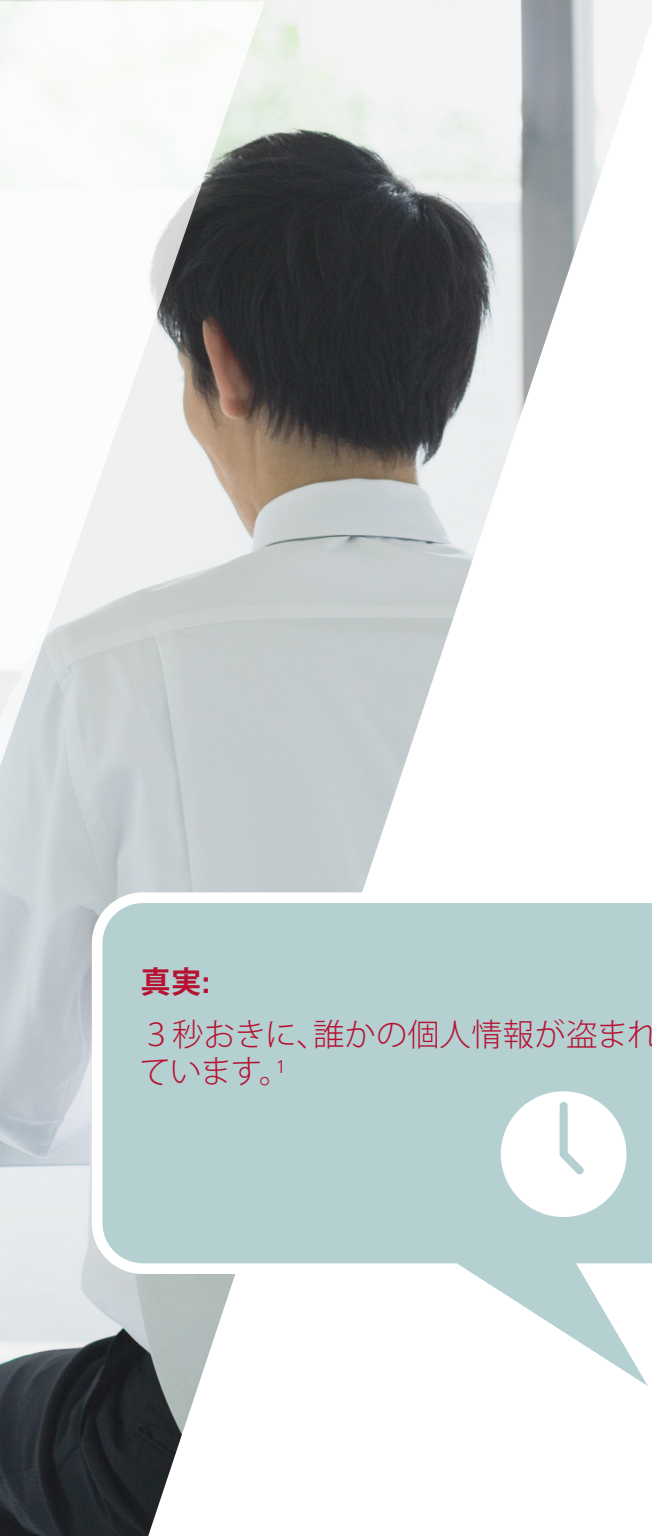
目次

はじめに

「泥棒」と言うと、持ち物が盗まれることを私たちは想像します。「泥棒」に遭わないように、私たちは自宅に警報装置を取り付けたり、貴重品を金庫や銀行にある貸金庫に預けたりします。しかし今日の場合、持ち物さえしっかり保護していれば安心、とはいかないようです。いまの社会の「泥棒」はまさにハイテク化しています。「泥棒」は、あなた自身の個人情報を盗み取ってお金を引き出し、クレジットカードを使い、あなた自身に対する評価そのものを破壊します。「個人情報泥棒」に遭う危険性はだれにでもあります。なぜなら、オンラインショッピングサイトや企業のデータベースだけでなく、財布、小さな紙切れなどあらゆるところに大切な個人情報が散らばっているからです。

本書では、個人情報の盗難が起きる仕組みと、これを防止する方法についてご紹介します。

個人情報の盗難とは

個人情報の盗難、あるいは身分詐称は、特定の個人を識別するための情報(名前、パスポート番号、銀行口座番号、クレジットカード番号など)をだれかが盗んだときに発生します。盗まれた情報は、その本人になりすまして利益を奪い取るために利用されます。利益には、銀行口座へのアクセスやクレジットカードの利用といった金銭的なものだけではなく、「泥棒」が犯罪を実行したり、特定の仕事に就くために利用する風評に関するものもあります。

個人情報は盗まれると、クレジットカードアカウントを開設したり、銀行口座の小切手を偽造したり、パスポートなどの公的文書を偽造したりするために利用されます。

このような事態が起きた場合、被害者はお金を失うだけではなく、ローンによる借り入れができなくなったり、医療保険給付を受けられなくなったり、更には信用を失ったり風評のために仕事に就けなくなったりすることもあります。また、ひどい場合には誤った個人情報のために逮捕されることもあります。

被害者は大抵、非常に長い時間が経過してからやっと個人情報の盗難に気付きますが、気付くのが遅すぎるために、泥棒はすでに近くにいません。こうした現実は、個人情報がいかに簡単に盗まれ、警察当局による犯人の追跡がいかに難しいかを示しています。

真実:

３秒おきに、誰かの個人情報が盗まれています。[1]

[1] 資料出所: Identity Theft Protection site (個人情報盗難防止サイト)、
http://identityprotectiononline.com/2009/07/10/identity-theft-statistics/

個人情報の盗難に関する重要な真実

- 米国ジャベリン社は身分詐称被害に関する 2010 年のレポートのなかで、米国の成人 1,110 万人が身分詐称の被害者であり、その規模は 2008 年の 12% 増、2007 年の 37% 増であることを発表しました。[2]

- 2008 年の米国の個人情報盗難による被害総額は 540 億ドル(約 5兆530 億円)に上ります。[3]

- 身分詐称被害者の 1 人当たりの平均被害額はおよそ 5,000ドル (約 47 万円)に上ります。[4]

- 個人情報の盗難から 6 ヶ月以上が経過してから気付いた被害者の損害額は平均的な被害者の 4 倍に上ります。[5]

- 2005 年から 2009 年までの間に、法人企業による情報漏えいが原因で 5 億人以上の消費者の個人情報、金融情報が公開されました。個人の安全対策では手の届かない場所で被害が起きてしまっているケースです。[6]

- 個人情報盗難の被害者は、既存の口座による損害の修復に平均で 58 時間を費やし、新しく開設された不正口座による損害の修復に平均で 165 時間を費やしています。[7]

- 個人情報の盗難の 43% は盗まれた財布、小切手帳、クレジットカード、請求書、またはその他の文書により発生しています。[8]

[2] 資料出所: Javelin Research & Strategy、*"2010 Identity Fraud Survey Report (2010年身分詐称被害に関する調査報告)"*
[3] 資料出所: 同上
[4] 資料出所: 同上
[5] 資料出所: Identity Theft Research Center (個人情報盗難防止研究センター)、*"Identity Theft: The Aftermath 2008 (個人情報の盗難: 2008年の被害状況)"*
[6] 資料出所: IdentityTheftInfo.com
[7] 資料出所: Identity Theft Research Center (個人情報盗難防止研究センター)、*"Identity Theft: The Aftermath 2008 (個人情報の盗難: 2008年の被害状況)"*
[8] 資料出所: 同上

個人情報の盗難のさまざまな姿

個人情報の盗難といえば、通常はクレジットカードや銀行情報の盗用をイメージしますが、実際には、健康保険や風評被害など私たちの生活に大きな影響をもたらす多種多様な個人情報の盗難があります。

ここでは、私たちが自分自身や家族を守るために必要な措置を更に理解できるようにするため、個人情報の盗難の様々な手口を紹介します。

金融関連の個人情報の盗難

金融関連の個人情報の盗難の場合、盗まれた個人情報は個人の預貯金やクレジットにアクセスするために利用されます。この手法はすぐに儲かるうえに追跡が難しいため、最も一般的な個人情報盗難の手口となっています。金融関連情報の盗難では、次のような被害が見られます。

- **クレジットカードの身に覚えのない支払請求** — クレジットカードを盗んだり、カード会社からの請求書の送り先を操作して個人情報を獲得した泥棒は、個人のクレジットアカウントそのものを横領して不正な支払に利用します。カード会社から郵送される新しいクレジットカードを勝手に受け取ったり、身分詐称により新しいクレジットカードの発行を依頼する、という方法もまた、個人のクレジットアカウントにアクセスするための手口として利用されます。盗用されたクレジットカードの支払いが滞ると被害者自身の信用が損なわれます。このような現象は、個人情報を盗まれていることにしばらく気付いていない場合に特に顕著です。
- **信用の悪化** — 個人情報泥棒が個人の身分を詐称して貸付金を利用したり、商品やサービスを獲得した後、返金や代金を支払わないと、その個人の信用は悪化します。

詐欺/身分詐称

個人情報窃盗/なりすまし犯罪は、泥棒が他人の個人情報を奪い、自分のものとして利用する場合に発生します。このような泥棒は、警察当局による取調べや逮捕時に、他人の運転免許書、生年月日、パスポート番号を名乗ります。また、詐称者はターゲットの個人情報を含む偽造運転免許証等を提示する場合もあります。

身分詐称犯罪では次のような被害が見られます。

- **犯罪歴** — 身分詐称者は、何らかの罪を犯してから他人の振りをしてその人の名前を警察当局に提示します。このような方法により、名前を利用された本人は犯してもいない罪の犯罪歴を持つことになり、逮捕状を発行される場合もあります。被害者は最終的に牢屋に送り込まれる危険もあります。
- **自分名義の交通規則違反や逮捕状** — 個人情報泥棒は他人の運転免許書を盗んで交通規則に違反し、取締り警官に対して他人に成り済ましてその人の運転免許書を提示します。個人情報泥棒がこの際の罰金を支払わなかったり、交通裁判所に出頭しなかった場合、名前を利用された被害者は更に重い罰金を請求されるか逮捕状を発行されます。

医療関連の個人情報の盗難

医療関連の個人情報の盗難は、他人に成り済まして治療薬を獲得したり医療保険給付金を請求します。これは最近もっとも急激に増えつつある盗難方法の 1 つです。医療保険給付金の請求額は、潜在的に何百、何千ドルにまで加算できる可能性があるため、このような手口を利用する泥棒の生活は劇的に改善します。

医療関連の個人情報の盗難では次のような被害が見られます。

- **保険給付の支払拒否** — 別の人が本人に成り済まして保険給付金をもらっている場合、個人情報を盗まれた本人は誤った医療記録がもとで自分の給付がもらえなくなったり、現在受けている治療も給付対象から外される可能性があります。
- **誤った治療** — 医療関連の個人情報は盗用されると、医師の手元には誤った情報に基づいて作成されたカルテが残ります。例えば、血液型やアレルギーの記録などが本人のものと違う場合、誤った治療によって重大な事故または死亡に繋がる危険があります。

個人情報はどのようにして盗まれるのか

個人情報の盗難問題はますます深刻になりつつあります。そこで、個人情報がどのようにして盗まれるのかについて知ることによって、問題解決に向けて少しでも前進する必要があります。しかし、残念ながらその手口は千差万別で、財布を盗む、郵便受けから手紙を盗み取るといった昔ながらの手口からデータ侵入や電子メール詐欺のようなハイテクを駆使した手口まで実に色々あります。

ここでは、いくつかのよく見かける手口を紹介し、貴重な情報を保護するためのヒントを学びましょう。

コンピュータを使った手口

- **フィッシング (Phishing)** — フィッシング詐欺は、サイバー犯罪者によって送信されるスパムメールであり、正規な機関等を装って個人情報の開示を要求します。例えば、サイバー犯罪者は取引銀行を装って個人に偽のメールを送信し、リンクをクリックして口座に関する情報を確認するよう求めます。このリンクは偽の Web サイトに連結しており、銀行口座やユーザー名、パスワードの入力を要求します。フィッシングは、サイバー犯罪の最も典型的な手口で、このような手口を使う泥棒は、相手から個人情報を騙し取るために頻繁に詐欺メールの内容を更新し、変更しています。
- **ファーミング (Pharming)** — ファーミングは、ハッカーが悪意のあるコードを個人のコンピュータに仕掛け、利用者に気付かれずに偽サイトへと誘導する手口です。この場合、個人は偽のショッピングサイトに誘導され、不正なサイトであることに気付かないまま支払い情報を入力してしまう危険性があります。
- **スピム (Spim)** — スピムは、インスタントメッセンジャー (IM) を利用して配信されるスパムです。インスタントメッセンジャーは、スパイウェア、キーロガー (keylogger)、ウイルス、そしてフィッシングサイトへのリンクを含む可能性があります。
- **スパイウェア (Spyware)** — スパイウェアは、コンピュータ利用者の個人情報を収集するために、ハッカーが無断で利用者のコンピュータにインストールするソフトウェアを指します。このソフトは、ユーザーを偽の Web サイトに誘導したり、設定を変更したり、その他の方法でコンピュータの制御権を奪い取るために使用されます。

- **キーロガー (Keylogger)** — キーロガーは、キーボードに打ち込んだ文字を記録する、スパイウェアの一種の形式です。打ち込んだ文字い関する情報は、ハッカーからアクセスできるファイルに保存されます。例えばコンピュータ利用者がインターネットで銀行サイトやお買い物サイトを開いたとき、キーロガーは口座情報やパスワード情報を記録します。ハッカーはこれらの情報を利用してコンピュータ利用者のクレジットカード情報や銀行口座情報にアクセスし、最終的には個人情報を盗用します。
- **トロイの木馬 (Trojan horse)** — トロイの木馬とは、無害に見えるように細工された、悪意のあるプログラムです。Web サイトから、トロイの木馬であることに気付かずにファイルをダウンロードすると、ハッカーは世界中どこからでもそのコンピュータにリモートアクセスできるようになります。これによりハッカーはコンピュータ上のファイルにアクセスできるだけでなく、ユーザーの画面操作をすべて観察できるようになります。
- **ソーシャルネットワーキングサイト (Social networking site)** — ソーシャルネットワーキングは大変人気がありますが、私達はこれを利用する際、グループの外にいる人達もソーシャルネットワーキングに掲示した個人情報にアクセスできるということを普段は忘れがちです。名前、生年月日、連絡先情報、会社等に関する情報をこのようなサイトに提供すると、個人情報泥棒は、個人情報を盗むために必要な情報を1つ1つ集め始められるようになります。
- **ウォードライビング (Wardriving)** — 個人情報泥棒は、ウォードライビングと呼ばれるテクニックを使って個人情報を盗み出す可能性もあります。これは、車で移動しながらセキュリティが脆弱なワイヤレス接続 (ネットワーク) を捜し求める手口です。自宅等で使用するワイヤレス接続のセキュリティが安全でない場合、ハッカーはワイヤレスルーターに接続されているすべてのコンピュータにアクセスできるようになり、銀行サイトやお買い物サイトに入力するクレジットカード情報等を盗み読みされます。

真実:

インターネット詐欺による個人識別情報の盗難件数は常に史上最高を記録しています。[9]

[9] 資料出所: Federal Trade Commission, *About Identity Theft* microsite

日常環境で使用される手口

- **郵便受け荒らし** — 個人情報泥棒は、郵便物を配達する振りをしながら郵便受けを物色します(通常は地方や郊外で発生)。目的は銀行口座等の情報を含むクレジットカード、銀行、その他の金融関連書類です。また、即時に使用を開始できるクレジットカードの申請書等もねらわれやすく、この書類があれば所有者に知られずにカードアカウントを作成できます。
- **ごみ箱あさり** — 都会では、ごみ箱の中身を物色して金融関連書類や重要な情報を含む資料を探し、個人情報を盗む泥棒もいます。個人情報泥棒は、郵便受け荒らしやごみ箱あさりにより獲得した情報を使って支払伝票等の送り先を変更し、個人情報を盗んだことが本人に気付かれないように細工します。
- **財布/小切手帳泥棒** — 財布や小切手帳の泥棒は最も原始的な方法のようですが、非常に効果的な方法です。大抵の人は運転免許書だけでなく、クレジットカードや 銀行カードを一緒に持ち合わせているため、なりすまし犯罪を行うために必要な情報がすべて泥棒の手に渡ってしまいます。
- **自宅から情報を盗む** — 私達は、家族や訪問者、自宅で働く従業員、工事業者等から見て簡単に手の届くところに請求書や重要な情報を放置しがちです。
- **不正な住所** — 個人情報泥棒はまた、簡単に個人の住所を変更してあらゆる貴重な手紙類を別の住所に転送させます。そして、そこから貴重な情報を盗んだり、銀行口座やクレジットカード口座の使用権を奪います。
- **ショルダーサーフィン** — 個人情報泥棒は、ターゲットの肩越しに ATM の使用やコンピュータのキー操作をのぞき見し、暗証番号やパスワードを盗み見します。また、個人が正規の業者に電話しているのを傍受して、クレジットカード番号や身分識別情報を盗み聞きします。いずれの場合でも、データがこのようにして個人情報泥棒の手に渡ると、重大な犯罪を実行される危険が発生します。

真実:

個人情報盗難事件の被害者の 42% が、なりすまし犯罪者が友人、家族、離婚前の夫/妻、或いは同僚のような親しい間柄の人であったと報告しています。[10]

[10] 資料出所: Federal Trade Commission, *About Identity Theft* microsite

真実:

ATM スキミングの手口による消費者と企業の被害額は年間 85 億ドル (約 7,900億円) を超えています。[11]

その他の手口

- **ビッシング/スミッシング (Vishing/smishing)** — ビッシングやスミッシングは、フィッシングとほぼ同じですが、ビッシングの場合は電話を利用し、スミッシングは **SMS** を使ったテキストメッセージを利用します。但し、両方とも電子メールコンポーネントを含む場合があります。

  ビッシングの場合、詐欺行為者は銀行からの電話を装って個人に電話をかけ、所有する口座に何らかの異状な手続きがあったと報告します。次に通話中に口座に関する詳細情報の確認を求めます。

  スミッシングの場合、詐欺行為者は悪意のある Web サイトへのリンクや電話番号を送信します。この電話には自動音声応答システム (ビッシングの類) が対応するようになっており、個人情報の入力を要求します。

- **スキミング (Skimming)** — ATM の機械に銀行カードを差込んだ場合や偽のカードリーダーにクレジットカードを挿入した場合、スキミングに遭う可能性があります。スキミングでは、ハッカーが銀行カードやクレジットカードの後ろの磁気テープを読み出して情報を獲得します。この情報を使うと、個人情報泥棒は他人の銀行口座にアクセスできるようになります。また他人の名前や詳細情報を含んだ偽のクレジットカードを作成できるようになります。

- **企業のデータ漏洩** — あらゆる規模の企業は、健康保険事業者、保険事業者、オンラインビジネス業者であるかどうかに関わらず、重要な顧客情報を数多く保有しています。このような情報がもしもハッキングに遭ったり、漏洩した場合、個人情報や金融関連情報を曝露される可能性があります。

[11] 資料出所: http://www.spamlaws.com/identity-theft-skimming

個人情報の盗難はなぜ困るのか

時計やステレオを盗まれる場合とは違って、個人情報盗難は時間的にも金銭的にも大きな犠牲が伴います。また、精神的にも大きなダメージを受ける可能性があります。個人情報の盗難は個人の人生や将来設計にどのような影響を与えるのか、ここではその例について見ていきましょう。

経済的な損失

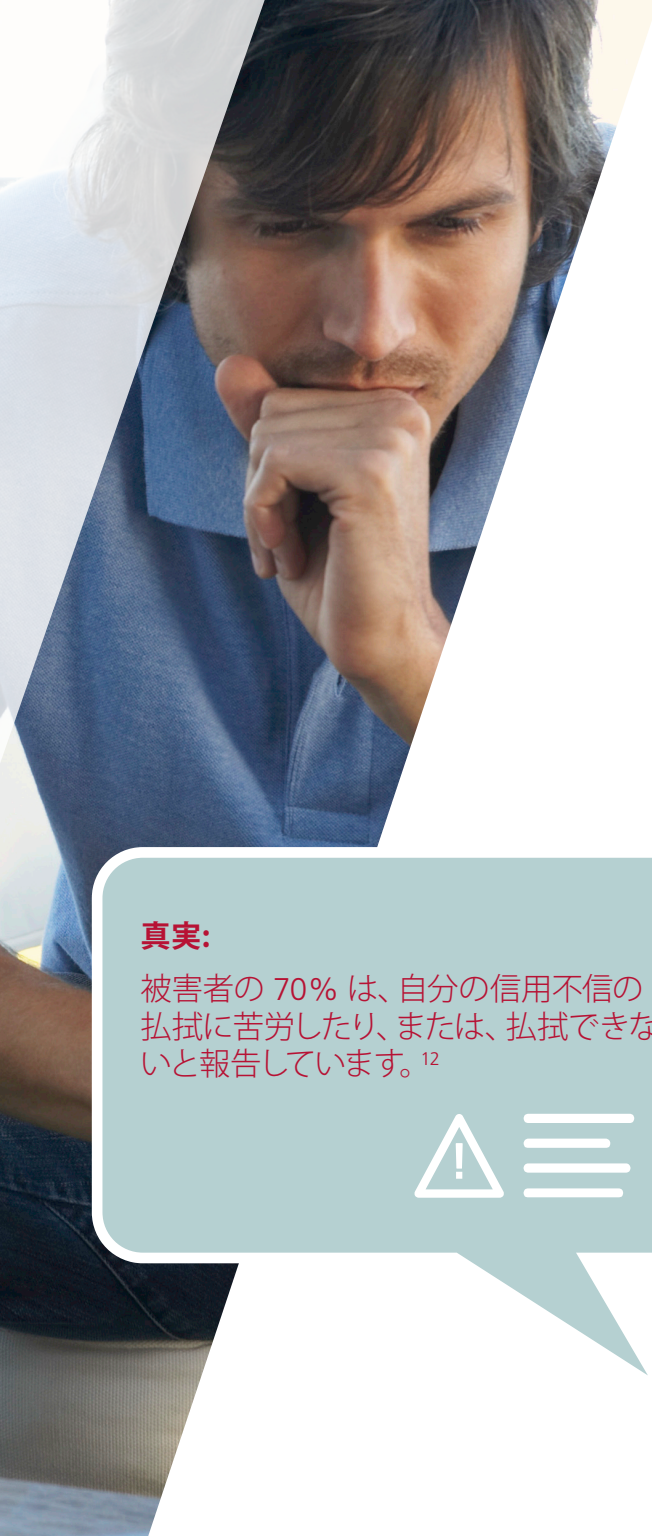
最もわかりやすいのは当然ながら金銭的な損失です。個人情報泥棒が、小切手、預貯金、投資口座等にアクセスできるようになると、口座から金銭を盗み取られる可能性があります。

信用の破壊

個人情報泥棒は偽の銀行口座を作ります。請求書も別の場所に送付させるため、本人の知らないところで利用限度額を超えて使い込む可能性があります。利用額の支払が滞ると、債務不履行口座という評価を本人の信用レポートに記載される可能性があります。しかし、こうして破壊された信用も、本人が自動車の分割払いや住宅ローンを申請して銀行側に拒否されるまで気付かない可能性があります。

信用の破壊は特に子どもの個人情報を盗まれた場合が危険です。なぜならこどもの場合、初めての金融取引を行い、信用を破壊されていることに気付くまでに数年を要するためです。

利益の損失

銀行口座情報だけでなく、パスポート番号や医療関連情報に関心のある個人情報泥棒も多く存在します。これらの情報を入手して、泥棒たちは本人になりすまして運転免許書を獲得し、利益を受け、就職する可能性さえあります。また、他人の医療情報を使い、医療保険給付対象となる治療を受ける場合もあります。彼らの受けた治療が年間の限度額を超えると、本人が実際に治療を受けたときに給付をもらえなくなる可能性があります。そして最も危険なのは、個人情報泥棒のカルテが本人のものと混同され、結果的に本人のカルテ情報を破棄される場合です。

犯罪歴

にわかには信じ難いことですが、個人情報泥棒は他人の個人情報を使用して罪を犯します。このため、本人にとっては身に覚えのない犯罪歴が付いてしまいます。泥棒は、他人の身分証明情報を使用するため、罪を犯した場合、犯罪歴は泥棒ではなく身分情報を盗まれた本人のものとして記録されます。そして、このときに犯罪を犯した犯人が罰金の支払を怠ったり裁判所に出頭しなかった場合は、裁判所が個人情報を盗まれた本人に対し、逮捕状を発行します。最悪の場合、本人は、交通違反によって自分が捕まるか、就職の際に行われる身元調査により不合格となった場合にやっとその事実を知ることとなります。

損失を修復するための費用

個人情報の盗難の被害者になったことに気付くまでには通常長い時間を要するため、損害額はどんどん積み重なっていく可能性があります。気付く前までに、複数の詐害料金が発生し、信用レポートを破壊され、ほかにも相当規模の修復作業や費用を要する問題が数多く発生している可能性があります。このような場合、数時間にわたって企業や政府機関に電話をかけて、問題を報告して自分自身の身分の潔白を訴える必要があります。また、金銭を支払って信用回復サービスを依頼する場合もあります。例えこのような場合でも、実際に本人の風評が元通りになるまでには数年を要する恐れがあります。

真実:

被害者の 70% は、自分の信用不信の払拭に苦労したり、または、払拭できないと報告しています。[12]

[12] 資料出所: http://www.spamlaws.com/id-theft-statistics.html

個人情報の盗難から身を守るには

一般的なヒント

- **警戒と教育** — 個人情報泥棒が個人情報を盗むために使う手段やだまし手口について知っておくと、個人情報の盗難に遭う危険性を大幅に減らすことができます。また、個人情報の共有については常に敏感になり、だまし手口等についても常に最新の情報を入手しておくと安心です。
- **一般知識** — 個人情報は、大切に保管しましょう。だれかから、または Web サイトや電子メールから個人情報の提供を依頼されたときは、このような情報を提供することが通常の手続きとして当然のことかどうかを念のため自問するようにしましょう。一般知識に照らしてよく考えると、銀行が電子メールを顧客に送信して口座番号やカードの暗証番号、ログイン用パスワードの確認を求めることが無いことに気付くはずです。
- **周りに人がいないかを注意する** — 電話で買い物をするときやATMの暗証番号を入力するとき、インターネットのお買い物サイトにクレジットカード情報を入力するとき、個人情報を書類に書き込むとき、身分証明のためにパスポート番号を使用するときなどは、周りに人がいないかを確認し、十分に注意します。

コンピュータと個人情報の盗難保護

- **オンライン保護** — インターネットを使って Web サイトを閲覧するときは、包括的なセキュリティ・ソフトウェアを使用しましょう。例えば、McAfee® Total Protection™ ソフトは、ウィルス、スパイウェアやその他の増大しつつある脅威だけでなく、個人情報の獲得を目的とした偽の Web サイトを検出して安全な検索技術を提供します。

  また、コンピュータではファイアウォールを設定して承認のない第三者のコンピュータがネットワークにアクセスできないようにブロックしましょう。

- **強力なパスワードを使用** — パスワードは、アルファベット、数字、特殊文字を混ぜ合わせて少なくとも 10 文字以上を使って設定します。また、パスワードは定期的に変更すると、個人情報泥棒が同じパスワードを使って不正使用し続けることを防止できます。パスワードは、家族や友達を含め、誰にも教えてはいけません。

- **公共の場所でインターネットを使用するときは安全なネットサーフィンを心がける** — 公共のコンピュータを利用したり、公共のワイヤレススポットやセキュリティで保護されていないワイヤレス接続を利用するときは、銀行サイトやクレジットカードサイトにログインしてはいけません。このようなサイトへは、自宅の安全なネットワークを使ってアクセスします。

- **自宅のワイヤレスネットワークの安全性を確保する** — ウォードライビングを防止するため、ルーターのファイアウォールを有効にして、管理者パスワードを変更しておきます。多くのルーターは、デフォルトのユーザー名とパスワードを備えています。これらの情報は最初にルーターを設置し、構成するため便宜上に与えれているものですが、ハッカーは通常このようなデフォルト情報に精通しています。また、ルーターのデフォルトの識別子を変更しておくほうが良い場合もあります。この識別子は付近のデバイスにルーターの存在を告知するために使用されるもので、ユーザーが指定したコンピュータやデバイスだけからのアクセスを許可します。お使いのルーターの取扱説明書を確認し、これらのデフォルト設定を変更する方法を確認しましょう。また、電子メールを使ってだれかにクレジットカード番号や銀行の口座情報を知らせることは絶対にやめましょう。

日常生活と個人情報盗難の保護

- **請求書類はこまめにチェック** — クレジットカードや銀行残高は毎月確認して、不正な支払等の発生が無いかを確認します。
- **書類をシュレッダーにかける** — ごみ袋の中から個人情報を盗まれないようにする唯一の方法は、財務書類やクレジットカードの勧誘、期限切れの身分証明書など重要な情報を含む書類をすべてシュレッダーにかけることです。
- **郵便受けにカギをつける** — 古くから使われているタイプの郵便受けの場合、個人情報泥棒は簡単に銀行書類や重要な金融書類を盗み出すことができます。
- **貴重な書類は大切に保管する** — 大切な個人情報を含む書類は鍵付きの引き出しや金庫、自宅のたんす等にしまいます。また、株券など更に重要な金融書類については銀行の貸し金庫に預けることも検討してください。
- **信用履歴を監視する** — 個人情報盗難の犠牲となった場合、その発見には通常長い時間を要するため、信用履歴は常に監視するようにし、使途不明な請求が発生していないかを常に注意しておく必要があります。自分の信用レポートに無料でアクセスさせてくれる Web サイトがいくつか存在します。また、信用情報の監視サービスを有料で実施するところもあります。
- **個人情報保護サービスを使用する** — 個人情報保護サービスは、個人の信用を監視することによって個人情報保護を支援し、自分の名前で新しい口座が作られた場合には通知を送信するなど、予防措置を提供します。こうしたサービスは通常、月毎に料金を徴収して提供され、これには信用レポートへの無料アクセスが含まれます。

被害に遭ってしまったら

個人情報を盗まれたことに気付いたときは、被害の拡大を防ぐためにすぐに対処しましょう。

1. **信用機関に通知して不正使用警告を作成する**
   信用機関の詐欺対策課に連絡して、状況を伝えます。担当者は、口座に対する不正使用警告を設定することができます。これにより、債権者は信用を供与する前に電話で本人に連絡をしてくれるようになります。

2. **警察に連絡する**
   個人情報を盗まれたことが分かっている場合は個人情報盗難について警察に届出ます。ここでは、不正利用される口座の一覧を作成してくれます。報告書のコピーを一部もらって、個人情報を盗まれたことの確認を求められたときに、債権者の調査担当者に配布できるようにします。

3. **口座によって影響される金融機関や公的機関に連絡する**
   銀行や債権者等に電話をかけて状況を連絡し、不正な請求や引き出しが行われた際には通知をもらえるようにします。電話で連絡を済ませたら、後で書面による正式な届出を行います。口座に対する請求が取除かれていることを確認し、必要に応じて口座を閉鎖します。盗難に関する情報についてはコピーを保管し、会話を文書化して記録を維持します。

4. **信用を凍結する**
   3つの信用機関で信用ファイルへのアクセスを凍結または閉鎖すると、泥棒が新しい口座を開くことを阻止できます。泥棒が新しい口座を作成しようとしたとき、信用を拒否されることになります。これは債権者またはサービスプロバイダが信用ファイルを確認できなくなるためです。

5. **法的な助けや個人情報修復専門家の助けを得ることも考慮する**
   損害があまりにも大きすぎて対処できない、という場合には債権回収者や信用機関、債権者との交渉について法的顧問に相談します。個人情報の修復専門家もまた、どのように問題を解決すべきかについて助言をしてくれます。

資料: 補足情報

以下の Web サイトは、個人情報の盗難や詐欺について更に理解を深め、保護対策を講じる際に役立ちます。

個人情報の盗難に関する情報

McAfee Cybercrime Response Unit (McAfee サイバー犯罪対応課)
http://www.mcafee.com/cru

Identity Theft Resource Center (個人情報盗難リソースセンター)
http://www.idtheftcenter.org/

Identity Theft Assistance Center (個人情報盗難防止支援センター)
http://www.identitytheftassistance.org

Privacy Right Clearinghouse (守秘権クリアリングハウス)
http://www.privacyrights.org/identity.htm

フィッシングの報告

Anti-Phishing Working Group (フィッシング対策ワークグループ)
reportphishing@antiphishing.org

Fraudwatch International (Fraudwatch インターナショナル)
scams@fraudwatchinternational.com

PhishTrackers.com (フィッシュトラッカーズ)
http://www.phishtrackers.com

コンピュータやインターネットセキュリティに関する更に詳しい情報については、下記のアドレスを通じてMcAfee Security Advice Center (McAfee セキュリティアドバイスセンター) にアクセスしてください。
home.mcafee.com/AdviceCenter/Default.aspx.

McAfee について

McAfee, Inc.は、米国カリフォルニア州サンタクララに本社を置く、セキュリティ技術の業界最先端の企業です。McAfeeは常に、世界で最も凶悪なセキュリティ脅威に容赦なく対処します。当社は、世界中のシステムおよびネットワークをセキュアにする画期的で優れたソリューションを提供しています。これらのソリューションにより、ユーザーは安全にインターネットに接続して Web サイトを閲覧し、安心してWebサイトを通じてお買い物をすることができます。受賞歴のある研究チームの力を通じて、McAfee ではホームユーザーだけでなく、ビジネスや公共機関、サービスプロバイダに対して革新的な製品を提供しています。これらの製品は、様々な規制に準拠しながらもデータを保護し、攻撃を防止して脆弱性を発見し、セキュリティを継続的に監視して改善します。

http://www.mcafee.com

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054   1.866.622.3911 www.mcafee.com

6665gde_identity-theft_0410